



SystemEDGE Recommended Configuration and Usage

In today's complex world of systems management, administrators need usage and configuration of SystemEDGE to provide the highest possible level of availability and fault management.

- **SystemEDGE
Best Practices**

Technical White Paper

Prepared by:
Russell Wynne
Engineering Product Manager
Version 1.0
March 25, 2002

Table of Contents

1.	Introduction.....	2
2.	Prerequisites.....	2
3.	Organization and Discipline a Key to Management.....	2
4.	General Configuration.....	3
5.	General Recommendations/Observations.....	5
6.	Logfile Monitoring Tricks/Suggestions.....	5
7.	Process/Service Monitoring Suggestions.....	7
8.	Alerting Strategies	7
9.	Security and SystemEDGE	8
9.1.	SystemEDGE Configuration for Security-Conscious Environments	9
9.2.	Privileged Access	9
10.	Extension Tips.....	10
11.	Working with other Management Software	10
12.	Other Resources.....	10

1. Introduction

SystemEDGE is a versatile SNMP and fault management agent for systems and applications. It increases the productivity of system administration support staff by enabling them to manage all UNIX and Windows NT systems on their networks from a single, central location.

SystemEDGE contains a plethora of features for monitoring various aspects of systems and applications, which power today's Internet infrastructure. System monitoring, process monitoring, and log file monitoring are a few of the features that can trigger alerts and start actions automatically from the system.

How these features are best utilized depends on the deployment, configuration, and operational choices made by the systems administrator. The object of this paper is to outline a set of best practices (not the only set) taken from our own usage as well as that of our users. While it is not the object of this paper to tell you exactly what to monitor, (i.e. what variables, what thresholds) We offer a number of obvious ones, (CPU, swap, memory, I/O, processes/services, etc.) along with some examples.

2. Prerequisites

This paper is not intended as a replacement for the documentation. The reader will need some familiarity with SystemEDGE features, capabilities, and supported platforms. The reader will also need familiarity with SystemEDGE installation and configuration. It will also be helpful to have a basic understanding of SNMP and systems administration concepts.

Note: This paper is not a substitute for the users guide, training, etc.

3. Organization and Discipline a Key to Management

While eHealth SystemEDGE, Application Insight Modules, AdvantEDGE View, and eHealth for Systems and Applications are designed to assist administrators, without proper discipline they won't be effective, or they may not even be successfully deployed. For example, deploying policy-based management can be a time-consuming and non-trivial pursuit. In many cases, that's because the policies weren't already in place before the deployment, and the deployment ends up involving internal political battles as these policies are defined. If the policies had already been in place, either manually or otherwise, the implementation would have been much easier and faster.

Managing desktops is another area where pre-existing discipline would smooth the process. Contrary to user beliefs, a company with 10,000 employees does not need 10,000 different desktop configurations. Standardizing to a few authorized desktop configurations would ease the administration of desktops. This concept holds true in systems management configurations as well. While variations may be necessary for different hardware and software configurations, they can be represented in a few standard configurations. This eases both the initial configuration and ongoing maintenance and support.

Some organizations go so far as locking down their configurations, and not allowing NOC users or general systems administrators to make any configuration changes. While I'm not necessarily advocating that, the chaos created by random, ad hoc configuration of systems is far worse.

Tips for establishing better IT processes and discipline:

- Procedures should be in place, and regularly executed, to keep management information current. Regular eHealth Discovery will ensure that polling is accurate and information will be available for all systems. It will also ensure that the system list for AdvantEDGE View is current.
- Managing by policy (whether done manually or automated) is simpler than managing individuals. This applies to systems management, security, etc. Think about managing by groups of similar devices, users, etc., rather than on an individual basis.
- Areas that seem to be out of control are good places to start looking for opportunities to streamline processes.
- Use Scheduling to automate tasks, especially the seemingly mundane ones, or they'll never get done. (Report generation, Discover, etc.)

4. General Configuration

SNMP port assignment

The industry standard is port 161. We also use 1691. 1691 is reserved with IANA (Internet Assigned Numbers Authority) for SystemEDGE use. Others should generally not be used. In both large and small environments, consistent port usage will aid in ease of use and ongoing management of SystemEDGE agents.

Reasons for consistent and standard port assignments:

- § Ports 161 and 1691 are standards.
- § Arbitrary port usage may conflict with other ports within systems.
- § Arbitrary port usage may cause additional work to configure for firewalls.
- § Arbitrary port usage will require special configuration of Network Management Systems.

Security?

Security is covered in more detail later in this document. However, the use of ports other than 161 or 1691 does not buy you that much in terms of security. Unique ports can still be found and SNMP packets can still be read. Other security measures are both appropriate and needed.

Community Strings

Community Strings are the most basic security feature of SNMP. Use of unique, non-English (or non-language) community strings is recommended. The Read-Only and Read-Create community strings should be different.

The Read-Only Community String should always be used for querying or polling SystemEDGE. The use of the Read-Create Community String for queries is discouraged for the simple fact that SNMP is sent in clear text and therefore not secure. The Read-Create Community String should only be used when necessary.

Grouping, Grouping, Grouping

Grouping is one of the primary keys to making SystemEDGE and all AIMs easy to manage and ultimately useful. In eHealth and AdvantEDGE View, systems can be added to multiple groups. Some ideas for groups include:

- System Type (i.e. NT, Solaris)
- Database Systems
- Clients
- Desktops
- Fileserver
- Email Servers
- Web Servers
- Application Relationship
- Physical Location

Configure by Group

Planning is one of the most important steps you can take in managing a large number of systems. Create template configuration files for each group/type. Create entries in the template for the specific application or services you are running. Include any actions or alerts.

Once the template configuration is complete, deploy it by copying the sysedge.cf file out to each system. Alternately, you can push the row entries out to the **group** through AdvantEDGE View.

Using a combination of basic templates and custom configuration is most common. First deploy the basic configuration. Monitoring the agent over time will provide the information needed to provide useful traps. As an example, the template threshold for CPU utilization may be 90%. But for some systems, 95% may be their operational norm for the applications they are running. These will generate needless traps. The threshold for these should be adjusted above 95% to be useful. (Live Health can and should be used to monitor for true deviation from normal.)

Standardize on a table of indices throughout the environment. Here is a sample of an index table:

Index Range		
Start	Stop	
10000	10999	Self Monitoring
11000	11999	Process Monitoring
12000	12999	Logfile Monitoring
13000	13999	NT Event Log Monitoring
14000	14999	History Table
15000	15999	Process Group Monitoring
16000	16999	Extensions (Regular)
17000	17999	Extensions (NT Reg/Perf Mon)
18000	19999	Service Response Indices
AIM Modules		
20000	40000	
20000	20999	IIS AIM
21000	21999	Apache AIM
22000	22999	Exchange AIM
23000	23999	Oracle AIM
24000	24999	SQL Server AIM
25000	25999	FireWall-1 AIM
Concord Reserved Index Ranges		
3000	3999	eHealth Service Response Paths

3000	3999	eHealth Process Monitoring
600000	699000	SystemEDGE Templates
600000	601999	Network Services Profile
1000000	1000999	eHealth System Template

Some hints for creating an indexing strategy

Each table has its own unique index space

- Reserve ranges for various types of settings
- Use large index numbers to allow for plenty of room for growth
- Standardize on index numbers for specific monitoring entries ie;
Row 10000 is always for CPU total idle monitoring
Row 12000 is always logfile monitor for SU failures

5. General Recommendations/Observations

Some general observations that will help in creating a useful, but generic set of entries to be used across multiple systems include:

- § CPU Utilization – Monitor Total CPU Utilization States (Allows the config to be portable across single and multiprocessor platforms)
- § Threshold monitoring – Start by configuring everything to send at-most-X traps with X=2 or 3. Otherwise, event flooding of the NMS is possible. (Live Health and Fault Manager don't require the use of this feature.)
- § Enable Clear Events – Clear events offers the ability to reset the event in the agent as well as resetting the status in an NMS.
- § Reduce Polling Impact - When managing a large enterprise network with hundreds or thousands of systems, polling each and every system for granular (less than 15 minute intervals) management information may not scale particularly well.
To save bandwidth you may be forced to:
 - o Place limits on what information is monitored
 - o Limit the poll rate
 - o Limit the number of systems you poll.
- § The unique self-monitoring capability incorporated into the SystemEDGE agent is specifically designed to provide the kind of granular, management-by-exception required for today's distributed network environments.
- § SystemEDGE also offers short-term history collection at the agent. This allows for the collection of very granular data (down to 30 second intervals). The history table can then be viewed as a graphical chart in AdvantEDGE View.

6. Logfile Monitoring Tricks/Suggestions

Logfile monitoring is one of the most powerful tools within SystemEDGE for turning system, application, and device events into SNMP traps and data. Monitoring system and application logs can offer the most in-depth look at application, user, and system behavior.

Included below are a sample set of monitoring entries that might be used for UNIX and NT. These by no means represent everything that can or even should be monitored on a particular system.

UNIX Basic Monitoring:

For a more detailed list of monitoring entries, please see the SystemEDGE Contrib Website:
<http://concord.com/sysedge-contrib>

Security Monitoring

Description	Logfile	Regular Expression
-------------	---------	--------------------

WARNING - daemon core	/var/log/daemon-log	core dumped
WARNING - daemon core	/var/log/syslog	core dumped
Monitor SU attempts	/var/adm/messages	su.*fail
Monitor slides	/var/log/daemon-log	slide
Monitor rlogins	/var/log/syslog	in.rlogin
Monitor telnets	/var/log/syslog	in.telnet
Monitor rsh	/var/log/syslog	in.rsh
WARNING - Illegal Instruction, Daemon	/var/log/daemon-log	.*illegal.*nstruction
Spam Relay Attempt	/var/log/syslog	Relaying denied

Device Failure Monitoring

Description	Logfile	Regular Expression
Critical: Badtrap Error	/var/adm/messages	.*BAD TRAP.*
Error: SCSI error	/var/adm/messages	.*SCSI.*[E,e]rror.*
Error: SCSI error	/var/adm/messages	.*SCSI.*failed.*
Error: SCSI error	/var/adm/messages	.*SCSI.*hung.*
Critical: badsimms error	/var/adm/messages	.*SIMM.*
Critical: badsimms error	/var/adm/messages	.*BAD.*SIMM.*
Critical: memory error	/var/adm/messages	.*[M,m]emory [E,e]rror.*
Error: disk error	/var/adm/messages	.*disk not responding.*
Error: disk error	/var/adm/messages	.*[D,d]isk.*[E,e]rror.*
'Warning: disk fragmentation error'	/var/adm/messages	.*optimization changed.*
Error: disk error	/var/adm/messages	.*corrupt label.*
Error: I/O error	/var/adm/messages	.*I/O.*[E,e]rror.*
Error: disk read/write errors	/var/adm/messages	.*Error for Command:.*[read,write].*
Error: media error	/var/adm/messages	.*Media Error.*
Info: serialport error	/var/adm/messages	.*zs[0,1,2]: silo overflow.*
Warning: carrier error	/var/adm/messages	.*no carrier.*
Warning: link is down	/var/adm/messages	.*Link Down - cable problem?.*
Error: SDS error	/var/adm/messages	.*[NOTICE,WARNING,PANIC]: md:.*

System Capacity Monitoring

Description	Logfile	Regular Expression
Critical: memory error	/var/adm/messages	.*[O,o]ut of [M,m]emory.*
Error: disk space error	/var/adm/messages	.*[F,f]ile system full.*
Error: disk space error	/var/adm/messages	.*No space left on device.*

NT

Security

Description	Event Log	Event Type	Description Filter (Regular Expression)
Random Password Hack	Security	All	.*bad
Misuse of Privileges	Security	All	.*[user rights,group management,security change,restart,shutdown]
Improper File Access	Security	Failure	.*[read,write]
Improper Printer Access	Security	Failure	.*print
Virus Outbreak Warning: program files updated	Security	All	.*write.*[exe,dll,com]
Security Policies Change	Application	Information	.*[S,s]ecurity policy

Application and System

Description	Event Log	Event Type	Description Filter Regular Expression)
Application Error or Failure	Application	All	.*[F,f]ail.*[E,e]rror
Application Load Problems	Application	All	.*[L,l]oad.*[P,p]roblem
New Software Installed	Application	All	.*[INSTALL,Install,install]
Server Process failed during Initialization	Application	All	.*4131
Disk Failures and errors	All	All	.*[D,d]isk
Network Adapter Errors	All	Error	.*[N,n]etwork [A,a]dapter

Monitoring a Logfile Size:

Set up logfile monitoring for a bogus expression and then threshold-monitor the logFileSize.x variable.

Rotating Logfiles:

When logfiles have a rotating name, use symbolic links to point a static filename to the current filename. If you write your own applications, don't write them to use logfile.timestamp; that's evil. Don't write applications that use fixed logfile size and circle within it. SystemEDGE cannot see where the file-pointer is inside file. Scheduled scripts can be used to update either the links or the SystemEDGE logfile monitoring entries to match the current logfile name.

7. Process/Service Monitoring Suggestions

Using SystemEDGE to monitor processes allows you to take burden off your staff, network management system, and your network. Use SystemEDGE to monitor critical processes. Should the process stop, or cross performance thresholds, the process can be stopped and/or restarted. It is also a good idea to send traps to the management system and may be prudent to send an email to the administrator of the process letting him know that a process has generated errors on the system.

Process and Service Monitoring should cover several aspects of an application. The following status and attributes should be considered:

- Process Liveness
- CPU Time Over Interval
(if non-incrementing, chances are high its in a zombie state)
- Too Much CPU Time
(Process Time delta for a threshold)
- Leaking Memory
(RSS graph over time and use alarm threshold)
- Auto-Restart a Failed or Zombie Process
(I tend not to auto-restart processes/services due to maintenance issue but many users like this feature.)
- On UNIX, application shutdown files can disable process/service monitoring to prevent race conditions.
- Use the Process Group Table for monitoring multiple processes with the same name.

8. Alerting Strategies

Alerting Strategies vary for site to site. However, one thing is common, managing the potentially massive flow of alerts is critical to every network and systems administrators success.

Push workload out to the agent for increased scalability

To limit the number of potential traps from a single monitoring entry, use the various flags provided in SystemEDGE.

- o Send Up To X Traps – allows only X traps to be sent to the NMS
- o Send Traps after X Events – simple time over threshold

Paging and emails can be sent from either the individual systems or the trap receiver. An example of a paging/email entries is:

Description: Web Server Process (httpd – on UNIX or WWW/Apache on Windows)
Interval: 30
Stype: Absolute
Attribute: 4
Operator: ==
Flags: 0x100 (monitor the parent process)
Action:

UNIX

/opt/EMPSysedge/contrib/email.unix -r mailserver server@here.com you@here.com 'Web process is down'

NT

C:\sysedge\contrib.\email.nt.exe -r mailserverserver@here.com you@here.com 'Web process is down'

The description field in a monitoring entry should be used to convey useful information. The description field is sent in an email notification as well as the trap. Useful information could include the priority or severity of the problem (critical, severe, minor, etc.) as well as nature of the problem. (Hard Disk Full, Application Stopped, etc.)

If you want to use traps to establish that SystemEDGE SNMP is up, you can set up a "heartbeat" by periodically monitoring numCPU > 0.

Trap Deduplication

Event deduplication strategies vary from NMS to NMS. However care should be taken not to deduplicate based on the wrong information. Some rules of thumb that will help are that most basic deduplication by NMS's are broken out of the box for SystemEDGE. You should not deduplicate based solely on trap type. (All logfile-monitoring entries would be lumped together.)

Deduplication of logfile monitoring traps and NT event monitoring traps should be based on source index number or matched string from within the trap.

Deduplication of NT-event monitoring traps should also be based on source index number or matched string.

When in doubt, deduplicate SystemEDGE traps by entry index number.

9. Security and SystemEDGE

SystemEDGE supports SNMPv1 (Simple Network Management Protocol version 1). SNMPv1 offers only basic security through community strings. *Community Strings* can be thought of as simple passwords that are required to access devices via SNMP. Because community strings in SNMPv1 are passed as clear-text, its usage must be done so with proper consideration.

In addition to the basic Community String security offered by SNMPv1, implementation of access-control lists within SystemEDGE, offer further security. Access-control lists allow network and system administrators to limit who can communicate with SystemEDGE agents. A separate community string and access-control list can be specified for Read and Read-Write operations to SystemEDGE. The Read-Only community string and access-control list specifies exactly which hosts

can perform SNMP Get operations. The Read-Write community string and access-control list specifies exactly which hosts can perform SNMP Get and SNMP Set operations. SystemEDGE also provides SNMP authentication failure Traps that warn administrators of attempts to access SystemEDGE with an incorrect or improper community string.

Prudent network security is essential to maintaining the usefulness of both community strings and access-control lists. Network administrators must limit the ability to “sniff” the network for traffic and prevent spoofing of network addresses. Traffic to port UDP/161, the standard SNMP Agent port, should be limited to the internal, trusted network. SNMP requests should not normally be allowed to transit through firewalls.

Some other helpful security hints:

- Use non-dictionary words to make communities harder to discern. (Make them look like random data.)
- Certain SystemEDGE functionality and MIB tables can selectively be disabled via configuration file keywords. (See Below)
- On UNIX, use separate user/group to run sub-programs for actions and extensions.

9.1. SystemEDGE Configuration for Security-Conscious Environments

In addition to the SNMP and access-control lists security mechanisms previously described, SystemEDGE provides several additional features for limiting the operations and access to certain data deemed sensitive to the security and integrity of the underlying system.

For sensitive installations, we recommend the following configuration file (sysedge.cf) options. Refer to the SystemEDGE User's Manual for complete details.

Command	Description
No_usergroup_table	Disables access to user and group information
No_who_table	Disables access to current user information
No_remoteshell_group	Disables use of remote shell access
No_process_sets	Disables set operations to the process table

Other options you may want to consider, depending on the particular deployment environment, are:

Command	Description
no_process_group	Disables access to running process information
no_actions	Disables use of actions
subprogram_user_name	Runs actions and extensions as a non-privileged user
subprogram_group_name	Runs actions and extensions as a non-privileged group

9.2. Privileged Access

SystemEDGE is designed and implemented to limit dependencies on external commands and programs. SystemEDGE does not invoke system commands on the underlying system to gather performance information. For example, SystemEDGE does not invoke the UNIX “ps” command to gather process information. Instead, SystemEDGE is implemented to gather the information directly from the kernel application programmer interfaces (APIs). This design greatly increases the efficiency of SystemEDGE, but is also important for security. There is no way for a user to reduce the integrity of the performance data by substituting a new version of the command or changing environmental variables like PATH and LD_LIBRARY_PATH.

However, in order to obtain complete performance information, SystemEDGE must be run as a privileged user: root on UNIX and system administrator on Windows NT. Since no commands are ever executed by the standard SystemEDGE configuration, the security risk is minimal. Using the above mentioned configuration options, the user can limit the available data to those items, which are strictly required.

10. Extension Tips

When creating SystemEDGE extensions, here are some tips to avoid pain.

- Use a separate MIB "spec" for listing extensions. Don't edit empire.asn1.
- Turn on SystemEDGE debug to troubleshoot. Use the logfile to find output, plugin, and extension problems.
- NT 128-character line-length limitation. Remember, NT only allows for command line entries to be 128 characters long. This includes paths, commands, and any arguments you may want to attach. The email action is a example: The call for the email executable and the included message can total no more than 128 characters. The excess will be truncated.
- Batch files are unreliable. Use Windows scripting, VBS, Perl, C, Shell, etc.
- Watch fork/exec time. When implementing new extension scripts or actions, keep in mind that extensions are synchronous and blocking. If a script hangs, no other actions will be performed until the action is cleared. (An upcoming release of SystemEDGE will allow for a timeout to be set for actions and clear this problem.)

11. Working with other Management Software

Some tips for working with Network Management Systems

- SystemEDGE is just SNMP V1.
- Most Management Systems allow you to import MIBs. Import the empire.asn1 and sometimes hostmib.asn1
- SystemEDGE supports MIB-2. Everything knows about MIB-2.
- Most Management Systems require trap definitions to be created. Save yourself some work and check out our "SystemEDGE Contributions" page for contributed definitions.
<http://www.empire.com/sysedge-contrib/>

12. Other Resources

- O'Reilly Book on SNMP (featuring SystemEDGE) written by SystemEDGE user
- eHealth SystemEDGE Users Guide
- Release Notes (With Each Distribution)
- SystemEDGE Contributions page
<http://www.empire.com/sysedge-contrib/>
- White Papers
http://concord.com/concon/sls_tools/tech_wp.asp
 - o SystemEDGE Licensing
 - o SystemEDGE Deployment
 - o SystemEDGE Security Issues
- SystemEDGE FAQ (http://concord.com/concon/inside/competitive/sysedgefaq_source.htm)
- MIB-2 (RFC-1213)
- Host Resources MIB (RFC 1514)
- Empire private-enterprise MIB (/EMPsysedge/docs - as installed with SystemEDGE)
- Book of Adrian (Sun Performance Tuning)
- Windows NT Resource Kit (3.51 version if possible, it has more info, and Latest for recent updates.)
- Mastering Regular Expressions (O'Reilly)